First Principles.

NATIONAL SECURITY AND CIVIL LIBERTIES

MAY 1976 VOL. 1, NO. 9 ESPIONAGE LAWS

In This Issue:

Coming: JUN.: FBI Charter

In The News

April 17, 1976 Rep. Bella Abzug, Chairperson of the House Subcommittee on Government Information and Civil Rights, made public a CIA statement revealing that over 60% of the agency's job applicants from 1963 through 1974 were rejected on the basis of polygraph (lie-detector) interviews. She has introduced legislation which would make it a criminal offense to administer polygraph tests in connection with federal government jobs. (*New York Times*, 4/18/76, p. 1.)

April 24, 1976 An FOIA suit has revealed that the contents of a briefcase stolen from the 1968 Socialist Workers Party presidential candidate, Fred Halstead, turned up in the hands of the FBI. Halstead believes FBI account —that the briefcase was found by an unidentified source and then surrendered to the FBI—to be a cover story. (*New York Times*, 4/25/76, p. 28)

April 29, 1976 On the basis of a 5-month review in the Department of Justice, Attorney General Levi announced that evidence was found indicating that the FBI undertook a systematic plan of harassment of Dr. Martin Luther King, Jr., but that there was no basis for believing that the Bureau either failed to make a thorough investigation of or was involved in his assassination. He ordered a second investigation by the Justice Department Office of Personal Responsibility.

In the Courts

April 2, 1976 *Weinstein v. Levi* (D.D.C. 2278-72) Order. In an FOIA suit for the Hiss papers, Chief Judge Jones issued an order requiring "a proper index accurately and separately describing in detailed, non-conclusory terms each and every document withheld from the plaintiff in whole or in part." With regard to material claimed to be exempt under the natural security exemption (b)(2) defendants are directed to provide "specific factual and evidentiary material accurately and adequately describing in non-conclusory terms the nature of the document, [proof of proper classification] . . . , and the reasons why it must continue to remain classified and at what level."

April 20, 1976 *Zweibon v. Mitchell*, No. 75-1056; *Barrett v. Zweibon*, No. 75-1046; *Mitchell v. Zweibon*, No. 75-1059. The Supreme Court declined to review a decision by the D.C. Circuit which held that warrants must be obtained for a government wiretap on a domestic organization that is neither the agent of, nor acting in collaboration with, a foreign power. The case, *Zweibon v. Mitchell*, 516 F.2d 594 (1975), now returns to the U.S. District Court for further proceedings.

It is at all times necessary, and more particularly so during the progress of a revolution and until right ideas confirm themselves by habit, that we frequently refresh our patriotism by reference to first principles.
THOMAS PAINE

In the Literature

Newspaper Articles

"Tapping Computers," by David Kahn, *New York Times*, 4/3/76, p. 27. The National Bureau of Standards, in cooperation with the National Security Agency, has proposed a "data encryption standard"—a common cipher to be used by companies putting their digital correspondence into secret form. Experts claim that, while the cipher is just strong enough to resist commercial attempts to break it, it is weak enough to yield to government cryptoanalysis, giving the government another opportunity to gain information from citizens' personal files at the expense of individual privacy.

Magazines

"Otis Pike and the CIA," by Oriana Fallaci, *The New Republic*, April 3, 1976, pp. 8-12. Interviewed with much "empathy," Chairman of the House Select Committee on Intelligence Pike relates his experiences in dealing with the CIA, Kissinger and the President while investigating the activities of the intelligence agencies.

"The Intelligence Tangle: The CIA and the FBI Face the Moment of Truth," by Sanford J. Ungar, *The Atlantic*, April 1976, pp. 31-42. *The Atlantic's* Washington editor examines the complex world of the United States intelligence community: its past activities, the recent congressional investigations, and proposals for reform.

"Annals of Law: Taking the Fifth," by Richard Harris, *The New Yorker*, Part I, April 5, 1976; II, April 12, 1976; III, April 19, 1976. A three part series detailing Fifth Amendment rights in their historical and present applications; covers grand juries, informers, immunity, etc.

PUBLICATIONS OF THE CONGRESSIONAL SELECT COMMITTEES ON INTELLIGENCE: A Bibliography

The House Select Committee on Intelligence (The Pike Committee)

The Select Committee's Investigation Record, in the *Village Voice*, February 16, 1976, pp. 70-92.

The Select Committee's Oversight Experience, in the *Village Voice*, February 23, 1976, pp. 60-68.

Available from *Village Voice*, 80 University Place, NY, NY 10003 — $1.80 per back issue.

Recommendations of the Final Report of the House Select Committee on Intelligence, by the House Select Committee on Intelligence, 94th Congress, 2d Session, Pursuant to H. Res. 591, February 11, 1976: House Report No. 94-833.

Senate Select Committee to Study Government Operations With Respect to Intelligence Activities (The Church Committee)

Final Report

Foreign and Military Intelligence, Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities, U.S. Senate, Book I, April 23, 1976, Report No. 94-755, $5.35.

Intelligence Activities and the Rights of Americans, Final Report, Book II, April 23, 1976, Report No. 94-755, $3.60.

These final reports provide a history of the evolution of intelligence, an evaluation of the intelligence system of the United States, a critique of its problems, recommendations for legislative action, and recommendations to the executive branch. The shortcomings of the intelligence system, the adverse effects of secrecy, and the failure of congressional oversight to assure adequate accountability for executive branch decisions concerning intelligence activities were major subjects of the inquiry.

Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Final Report, Book III, May 30, 1976, Report No. 94-755 (#69-984). Includes reports on COINTELPRO, FBI and Black Panther Party, Dr. Martin Luther King, Mail Opening, Warrantless Electronic Surveillance, Informers, "Black Bag" Break-ins, FBI Domestic Intelligence Investigations, IRS, NSA Surveillance, Military Surveillance, CHAOS, the Huston Plan.

Reports

"Alleged Assassination Plots Involving Foreign Leaders," examines U.S. involvement in assassination plots. November 20, 1975, #61-985-9.

"Covert Action in Chile, 1963-1973," December 18, 1975 (Staff Report). Available from the Committee: Dirksen Bldg. 308, Washington, DC 20510.

Hearings

Vol. 1, "Unauthorized Storage of Toxic Agents," September 16, 1975 #63-561-0, $2.45
Vol. 2, "Huston Plan," September 23, 24, 25, 1975, #62-685-0, $4.00
Vol. 3, "Internal Revenue Service," October 2, 1975, #60-877-0, $2.00
Vol. 4, "Mail Opening," October 21, 22, 24, #64-663-0, $2.40
Vol. 5, "National Security Agency and Fourth Amendment Rights," October 29, November 6, 1975, #67-522, $2.30
Vol. 6, "Federal Bureau of Investigation," November 18, 19, December 2, 3, 9, 10, 11, 1975, #66-077-0, $7.40

The Espionage Laws: In Need of Reform

BY CHRISTINE M. MARWICK

Introduction

The espionage laws which are currently on the books are ambiguous in their most basic elements — it is unclear precisely what kind of activities they mean to prohibit, and it is equally unclear what kinds of contribution to public debate on issues of defense policy citizens can safely make.

It was not until the trial of Daniel Ellsberg and Anthony Russo that the government took advantage of the ambiguity in the laws and used them against defendants who were not the alleged agents of a foreign power. Since the Ellsberg/Russo case was thrown out of court for government misconduct before the legal issues were resolved, the expansive interpretation of the espionage statutes has not been overturned. The administration is proceeding as if its preferred, highly restrictive interpretation of the statutes were good law: another espionage case has been brought, *U.S. v. Grunden*, AMC 21679, again without alleging intent to harm the national defense.

Although the Justice Department is prepared to use new and strained interpretations of the espionage statutes, the administration's preferred course of action would be to enact its preferences in the espionage provisions of S.1, the bill to reform the federal criminal code. The administration has been pushing S.1's espionage chapter as if it were little more than a codification of present espionage law, rather than an unprecedented incursion into political debate. Its language is drawn so broadly that the only legitimate source of information on national security policy would be official releases of the government. S.1 clears up any ambiguities only by making such broad restrictions that its espionage provisions would almost certainly be unconstitutional.

And the conservative Senate Judiciary Committee's report on the S.1 espionage proposals has accepted the administration's interpretation of current law, which includes provisions for

> *deterring conduct which might expose material to foreign eyes rather than against active espionage on behalf of foreigners.*

These interpretations do not respond either to First Amendment values or to the public's right to be informed. The executive branch is trying to call publication — or at least the actions which necessarily lead up to it — espionage. The Russians, the reasoning goes, can read the newspapers. But such a definition ends up treating the American public as tantamount to being a foreign power. And if it is unfortunate that the Soviets read the newspapers, it is also absurd for the public to be regarded as Soviet agents.

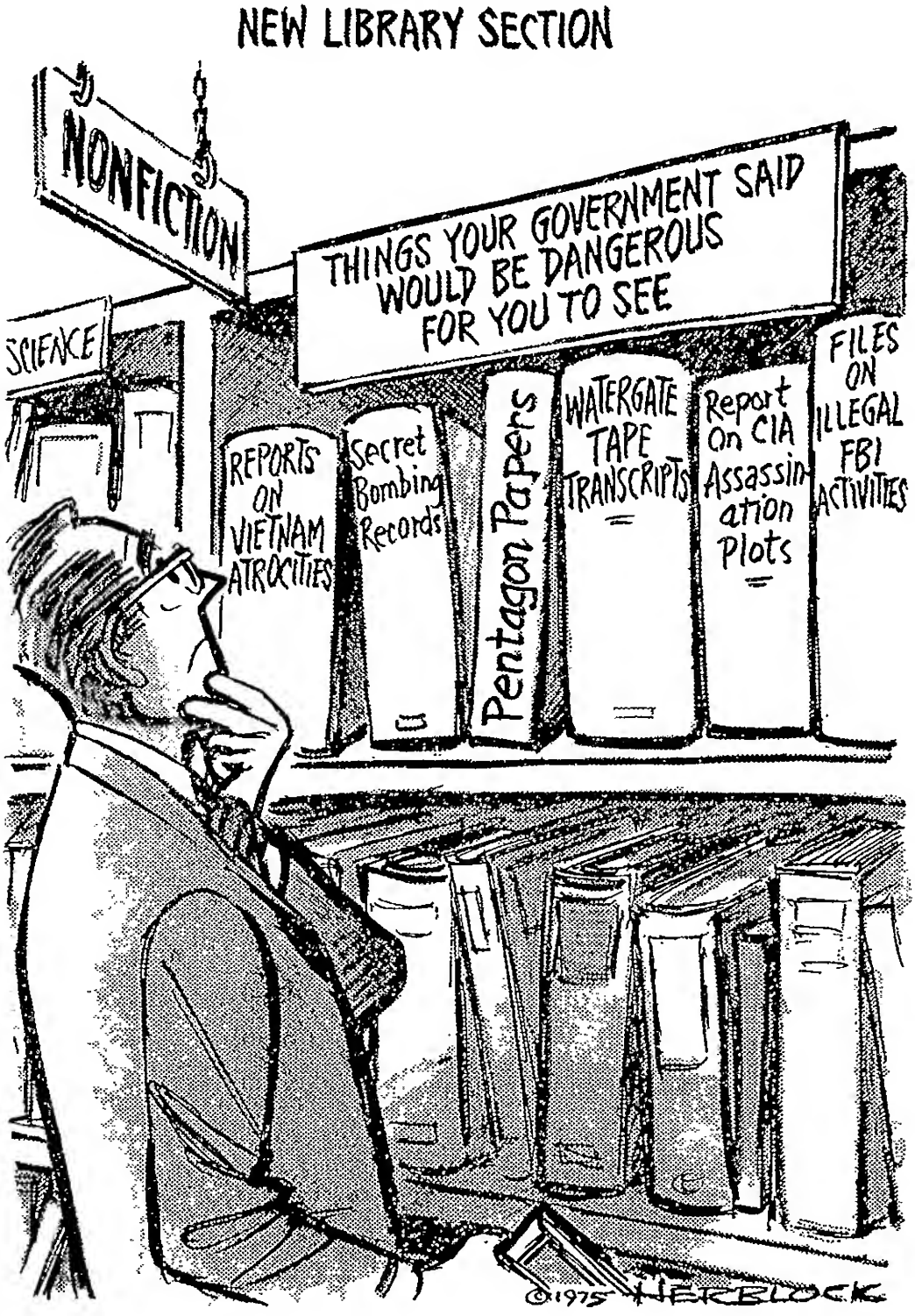
When Congress drafted the basic version of the espionage laws in 1917, they made it clear that they did not want to give the Wilson Administration the right to censorship and to conduct the war effort without criticism; they referred repeatedly to the British legal situation, which produced such anomalies as Lord Northcliffe's risking prosecution by revealing that British soldiers were being killed because of shoddy munitions. Congress's result, however, was an inadvertently ambiguous body of laws. The courts have repeatedly had to return to the legislative history to try to determine what was meant by the statutory language.

And in spite of the view preferred by the advocates of concentrated executive branch power, the fact remains that the First Amendment rights are not in conflict with the national defense; freedom of speech and of the press serve vital critical functions. It is not difficult to argue that the post-war system of closed national security decision-making has produced major policy disasters and that the rational response is to design a system which balances the need for open, critical discussion against the very limited actual needs for some secrecy.

There is now also the clear record that national security secrecy claims have been the most efficient tool for cover-up of political and policy scandals. But even if the classification stamp were magically limited from now on to only its good faith applications, there would still be the acknowledged fact of massive overclassification. Bureaucrats normally overestimate the importance of the information they deal with and underestimate the importance of outside criticism.

Yet even after being caught in a web of failures, the executive branch has been reluctant to change its assumptions. The government response to the Pentagon Papers furor was not to change its policies but to use strained new interpretations of the espionage laws in order to tighten control of information so that they could continue to shape policy debate.

It should be clear that trusting prosecutorial discretion



to limit indictments to espionage agents and to refrain from playing politics with a temptingly ambiguous criminal statute is not going to work; the First Amendment deserves better safeguards. Likewise, it places an unnecessary burden on the courts to ask them to sift through the motivations of not only the accused, but of the prosecution as well. Such a situation needs reform.

Coming in the wake of Vietnam and Watergate, it has been difficult to sell the need for S.1's provisions on behalf of unquestioned secrecy. The espionage provisions of the bill have been one of its most controversial features and one which has been bargained away in an effort to get the bill passed in this session of Congress. Senate Majority Leader Mike Mansfield and Minority Leader Hugh Scott sent a joint letter on February 11th to the Judiciary Committee members suggesting that the espionage chapter and other controversial provisions be removed, and that present law on the subject be allowed to stand. Senators McClellan and Hruska, the S.1 sponsors, rejected a Kennedy-Hart-Abourezk proposal that Sen. Philip Hart's amendments replace current law on the subject; instead, the compromise was reached that current law on the subject stand.

But the current law, with the Justice Department's present interpretation of its meaning, is far from innocuous. There is nothing to prevent its being used again in selective prosecutions to chill the freedom of the press. The question at issue now is not whether bona fide spies should be brought to justice, which the current laws provide for, but whether to allow a system which — intentionally or unintentionally, by new law or by executive gloss — cuts off information which the Congress and the public have a vital interest in knowing.

The Espionage Statutes

Before discussing the tension between the espionage statutes and the First Amendment's protection of a free press, we offer a very brief listing of some of the current statutes which relate to publication. For an exhaustive analysis of the statutes' language, legislative history, and case law, see "The Espionage Statutes and Publication of Defense Information," by Harold Edgar and Benno C. Schmidt, Jr., 73 *Colum. L. Rev.* 930 (May 1973).

18 U.S.C. §794(a) and (b). These subsections of the espionage chapter cover what is traditionally thought of as spying. §794(a) prohibits communicating "information relating to the national defense" "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation." §794(b) is more narrowly drawn — in time of war, it prohibits intentionally communicating (which specifically includes publishing) to the enemy information about the public defense, particularly troop movements, which might be useful to the enemy.

18 U.S.C. §793 deals with the control of information and differs from §794 in that it does not require proving criminal intent. Subsections (a) and (b) refer not to publication, but to obtaining military or national defense information or documents. Subsections 793(c), (d), and (e) are the statutes under which Daniel Ellsberg and Anthony Russo were indicted.

Subsection (c) makes criminal receiving or obtaining documents relating to the national defense if the subject has knowledge or reason to believe that the information will be "disposed of . . . contrary to the provisions. . ." of the espionage chapter.

Subsections 793(d) and (e) are those which pose the greatest threat to publication. Subsection (d) covers persons who are in authorized possession of such national defense information; subsection (e) covers everyone else. They make no special mention of the press, but as written they may be interpreted to prohibit both giving any written or oral information relating to the national defense to journalists and journalists retaining that information. These subsections are of sweeping breadth; without any special intent to injure the defense of the United States, they can be interpreted to make leakers, reporters, and memoir writers serious criminal offenders. The statute is virtually without workable limitations — taken to their logical conclusion, retaining one's memories can be illegal.

All the statutes of the espionage chapter are confusing, but (d) and (e) more so than the others. For instance, the legislative history of the statutes shows that Congress intended to exempt ordinary publications from the espionage penalties, yet these statutes, read literally, would make a newspaper's simple possession of documents illegal.

Other Espionage Statutes. There are several other statutes which are not treated in this discussion, but which provide an interesting contrast because, by comparison they are very specific about the kinds of information and communication they deal with. 18 U.S.C. §798 protects cryptographic information from publication; 18 U.S.C. §952 makes illegal the revelation by federal employees of information that has been transmitted in the code of a foreign country; 42 U.S.C. §§2271-81 protects information about atomic weapons or atomic energy and authorizes injunctions against publication; and 50 U.S.C. §783(b) prohibits federal employees passing classified information to foreign agents or members of the communist party.

Current Espionage Law: In Confusion

Different Kinds of Unofficial Release

In spite of the executive branch's efforts to the contrary, not all release of information without official blessing can be called espionage. Spies are not protected by the First Amendment, but if a democratic process is to function the public must be able to make informed judgments about national security policies. As written, the current statutes lump into one amorphous mass three different kinds of unauthorized release of information: espionage in the traditional sense, leaking, and publication. The laws do not allow the individual to determine clearly whether his or her action is merely adding to the public debate, or whether it crosses over into espionage and will bring down criminal sanctions. As written, and as the administration would use them, they can be interpreted to stifle political debate. Thus far, the courts have saved the espionage laws from being declared unconstitutionally vague by adding a gloss of judicial interpretations which have limited their overbreadth.

The three ways of releasing information must be distinguished if the laws which are designed to protect the nation do not end up stifling its political debate.

To begin, an effective espionage statute should offer a better characterization of spying, one that takes into account that the goal is to transmit information to a foreign government and the expectation is that the information will be used to injure the United States. Prohibiting espionage is not difficult — the only problem is that such a law should be drawn precisely enough that its sanctions do not bleed over into the other activities, leaking and publication.

The leaking "problem" is the subject of more dispute. Leaks perform a necessary function in the government; no one seriously denies that overclassification is endemic or that classification stamps have been used with a cynical facility to conceal a wide range of information which has nothing to do with the security of the United States. And Congress itself is aware that it relies extensively on leaks to find out what is going on in the executive branch, and has repeatedly declined to criminalize leaking. Before the Ellsberg case the executive branch decided not to prosecute what it considered serious leaks because it did not believe that the statutes allowed it unless there was a clear indication of culpable intent — espionage in the traditional sense.

If an anti-leak statute were strictly enforced, it would lead to over-deterrence — most leaks are neither serious nor even of particularly controversial information. There would generally be the feeling that invoking criminal sanctions would be inappropriately harsh, and given the generally high status of leakers, prosecution would instead be very rare but politically selective. As it is, the most effective deterrent remains the officials' concern for their careers. But in any event, most leakers would expect to escape detection, just as they do now. And such laws should not deter people who are acting as a matter of conscience.

But the effects on the body politic of an anti-leaking law are especially grim. There is no exception in the First Amendment which denies public servants their right to speak to policy questions or which authorizes cutting off this vital source of information for public debate. Without leaks, the policy making process would be the exclusive preserve of isolated offices in the executive branch.

The Ellsberg case was the first espionage case related to publication — although, as discussed below, the government avoided the publication issue and prosecuted only the activities which were necessary prior to publication.

The publication of the Pentagon Papers themselves was a rather confused affair as related to espionage. The government originally took the New York Times into court in an effort to restrain publication, and cited the espionage laws. However, the Judge ruled that the statutes did not apply; the case when to the Supreme Court on the basis of the catch-all for executive authority — "inherent presidential power." That Court produced mixed results on whether, given the statutes, such publication might constitute espionage; but the possibility of an espionage indictment after publication was seen as less serious threat to the First Amendment than the effort of the executive branch, without any grant of such authority from Congress, to install prior restraints on publication.

In any event, no journalists have been indicted and there is no case law which would clearly put publishing with intent to inform the public, rather than intent to transmit information to a foreign power, beyond the pale of a criminal indictment. This is due primarily to the fact that journalists have traditionally been highly cooperative rather than adversarial with the government, even in the post-Vietnam War and post-Watergate eras. The CIA, for example, very nearly managed to suppress the story of the Glomar Explorer; we have no idea how many stories have been successfully suppressed with press cooperation. Yet, it is not the press's job to help the government keep its secrets, but to contribute to public debate on policy issues.

The espionage laws say little about publication. Except for 794(b), which prohibits wartime publication about troop movements, sections 793 and 794 were not meant by Congress to apply to publication or to acts preceding it, but the language of the statutes is more vague than the intent shown in the legislative history. The government has claimed that the 1917 laws applied to general publication and discussion. Congress, however, found it necessary to later enact laws which protected diplomatic communications, codes, and Atomic secrets; it seems that they did not feel that sections 793 and 794 could in fact protect the nation from publication of these particular areas of communication. And, in fact, when dealing with legislation to protect cryptographic systems and communication intelligence activities, they said as much:

> *. . . unauthorized revelation of information of this kind can be penalized only if it can be proved that the person making the revelation did so with an intent to injure the United States. (H. Rep. 1895, 81st Cong., 2d Sess., April 6, 1950, p. 2.)*

A law which is designed to protect the nation from clandestine traffic in secrets should not be phrased so expansively that an administration confronted with vocal critics can use the statutes to subvert healthy debate. The current laws need to be revised to reaffirm and protect the public's right to information.

Ambiguity

In addition to fuzzy thinking about what kinds of communication the statutes should control, the terms of the statutes are highly ambiguous.

There are three elements of espionage: 1) the kind of information it covers, 2) the intent of the person who passes the information, whether to stimulate policy debate or harm the United States, and 3) who is to receive the information, whether it is the U.S. public or a foreign nation. Espionage convictions should be based on all three elements, yet all three elements are vague and expansive in current law. Undefined catch phrases such as "related to the national defense," "intent or reason to believe," and "not entitled to receive," run throughout the statutes.

"Information Related to the National Defense"

The espionage statutes are meant to control information which relates to the national defense, but Congress failed to explain how the individual is supposed to figure precisely where a discussion of policy might end and an illegal transmission of "defense" information begins. The breadth of this term is an invitation to declare it void for vagueness under the due process clause of the constitution.

The courts have recognized the dangerous breadth of the term — national defense information can mean virtually everything about a nation. In modern warfare, as Judge Learned Hand noted in *U.S. v. Heine*, 151 F.2d 813 (2d Cir. 1945), *cert. denied*, 328 U.S. 833 (1946), the most mundane economic and technological factors contribute to the national defense. In *Gorin v. U.S.*, 312 U.S. 19 (1941), Justice Reed accepted the government's definition — that national defense "is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness." So sweeping a definition makes it unclear what, if anything, anyone is entitled to discuss about military matters, and such vagueness invites selective prosecution against critics of government policy. The legislative history implies that Congress was relying on the "honorable man" theory — that even if the terms were perhaps a little nebulous, prosecutors would be relied upon to indict only in those situations which really deserved it. But it is the duty of the prosecutor to look for violations of the law, not to judge them, and it is asking a great deal to expect prosecutors to distinguish between an agency-ordained secrecy which is actually there to protect the national security and that secrecy which is designed to protect the agency's image.

Classification Stamps. "When everything is classified, then nothing is classified . . . ," wrote Justice Stewart in the Pentagon Papers prior restraint case (*New York TImes v. U.S.*, 403 U.S. 713, 729 (1971).) Even if the executive had been given the authority to back up the classification system with the espionage statutes, by the mere fact of massive overclassification the executive branch has effectively eliminated classification as a possible criteria for determining what is national defense information. Classification stamps do not help narrow the breadth of national defense information to a manageable scope.

Congress has repeatedly declined to make the unauthorized disclosure of classified information a crime. And in cases dealing with private citizens, classification stamps in themselves have been found not to determine whether a document is information related to the national defense. The jury is instructed that it is their role, not the role of the agency which stamped the documents, to determine whether information does in fact relate to the national defense and, therefore, the guilt or innocence of the accused which hinges on that. [See *U.S. v. Drummond*, 354 F.2d 132 (2d Cir. 1965), *cert. denied*, 384 U.S. 1013 (1966)]. In the Ellsberg case, Judge Bryne ruled that the government had to prove both that the Pentagon Papers had been properly classified using the correct procedures and that their substance was in fact classifiable.

There is only one statute which allows prosecution based on the simple fact of classification — 50 U.S.C. §783(b), which applies to government employees passing classified documents to foreign agents or communists. As interpreted in *U.S. v. Scarbeck*, 317 F.2d 546 (D.D.C. 1962), *cert. denied*, 374 U.S. 856 (1963), the statute does not require either that the information has been properly classified or that the defendant had a culpable intent. But even the *Scarbeck* statute has its difficulties in interpretation. For instance, unless stamped documents have actually changed hands, it would be difficult to prove that the particular information was classified and known by the accused to be classified, or whether the information came from the public domain.

Information in the Public Domain. The statutes have neglected to make a distinction between "secret" and "public" information, and the courts have tried to remedy this failing. In *Gorin* the Court found that collecting information which the government itself had actually put into the public domain could not be considered espionage: "where there is no occasion for secrecy . . . there can, of course, in all likelihood be no reasonable intent to give advantage to a foreign government." (312 U.S. at 28.)

And in *U.S. v. Heine*, the court held that collecting public information and even passing it to agents could not be considered "national defense information" within the meaning of the espionage law. To do otherwise, the court held, would threaten "drastic . . . repression of the free exchange of information . . . [and] extravagant and absurd consequences."

The Ellsberg trial has placed a different twist on the problem of national defense information in the public domain. The Pentagon Papers did carry classification stamps, and the prosecution contended that all that was necessary for information to be "related to the national defense" was for it to be contained in a classified document. But this position ignores the fact of overclassification — most of the information which appears in classified documents is already in the public domain in some form. And as the *Heine* court pointed out, if an individual can be brought to trial for communicating about publicly known information, it could literally mean the end of free speech concerning national defense policy.

The Ellsberg defense maintained first that if the information existed in the public domain as well as under a classification stamp, transfer of the classified document containing that information could not be criminal, and, second, that there was nothing in the historical study which was actually a secret. The government countered, in effect, that the study was greater than the sum of its parts, and that the information as a whole — all 46 volumes, including those which had not been involved in the transfer to Russo — met the standards of the statute's term, "national defense information." Judge Byrne supported the defense's position, and ruled that the jury must be allowed to determine for itself whether the information was public or secret national defense information.

Culpability

The second element of espionage is criminal intent, or culpability. Since the term "national defense" is so broad that it can mean virtually anything, the espionage statutes threaten to run afoul of the constitutional doctrine that a law must give the individual a fair warning of what specifically is prohibited.

Scienter. The Supreme Court has rescued the statutes from being declared unconstitutional by an interpretation based on scienter, or knowledge, arising from the accused's culpability or intent. If the defendant acts "with intent or reason to believe" that the information would "be used to the injury of the United States or to the advantage of a foreign nation," then it must have been understood that the information "related to the national defense" and that the conduct was criminal.

But this "clarification" sets the espionage statutes on

another track of ambiguities. Obviously, proving someone's psychological state — that the action was motivated by an intent to injure rather than by ignorance — is difficult at best. It is far easier to convict because of an intention to give "advantage to a foreign nation." Advantage has been interpreted as meaning "helpful," and since it is helpful to know as much as possible about another nation (whether friendly or hostile), the range of culpable communications of national defense information is broad indeed. In *Gorin*, the defense asserted that the information, while secret, was so trivial that it fell beyond the meaning of the statute. At this point, the "reason to believe" phrase came into play; Gorin was not allowed to be too stupid or ill-informed of the possible uses of seemingly trivial information which might make it helpful to a foreign nation.

Publication. The question of intent is most complicated in regard to publication of information in the American press. While someone who sells information to a foreign agent has reason to believe that some harm to the U.S. or advantage to a foreign nation will follow, publishing the information is done with the intention that it will inform the public; therefore the release of that information sidesteps the scienter requirement. The "reason to believe" standard produces more of a problem, however, since under *Gorin* it seems to require considerable sophistication about the possible applications of the information. No where does the statute allow balancing the possible advantage to the American people against the value of the possible advantage to a foreign nation.

The legislative history, indicates that the statutes were not intended to be used against publication. And indeed, to return to the case of Lord Northcliffe which was in the minds of the legislators, the public should know that the munitions are defective; the need for public outcry to remedy such a situation is more important than the advantage given to the enemy by confirming its tactical advantage.

Willfully. The language of 793(d) and (e), under which Ellsberg and Russo were indicted, adds yet another layer of ambiguity to the problem of figuring out what Congress actually intended to prohibit. Rather than the somewhat clearer standard of "intent or reason to believe", these subsections require only that the national defense information be "willfully" transmitted to someone "not entitled to receive." They give no clue, however, to what "willfully" might mean. Does it require, for example, that the transfer be motivated by some sort of anti-U.S. pique, an intent to harm the U.S. or help a foreign nation? Or is mere knowing recklessness enough to bring conviction? And if the national defense information which is transferred is not necessarily information which would cause injury/advantage, how is the individual to know just what is the scope of the information that one should not "willfully" transmit?

In 793(d) and (e) the scienter which rescued the constitutionality of the other espionage statutes must somehow be drawn from an interpretation of the word "willfully." The Ellsberg defense maintained that if the prosecution could not prove intent, which would reinstate the scienter, the statute would be unconstitutionally vague.

Judge Byrne tentatively concluded that "willful" meant that the government must prove that the defendant knew that the information related to the national defense and that it was given to a person who was in fact not entitled to receive it. Under this interpretation, the "willful" transfer of the information would pass the test of constitutionality only if the government were able to make the case that the other terms of the statute were specific enough to counterbalance the ambiguity of the stipulation "willful."

The Recipient of the Information

The third ingredient in espionage is the recipient. No one has claimed that a Soviet agent is entitled to receive national defense information, and the problem of defining more precisely who is not entitled to receive the information did not come up in the case law until Ellsberg.

But if the person who receives the information is not a foreign agent but intends to use the information to stimulate public debate, the statute must be reconciled with the First Amendment.

"Not Entitled to Receive." Subsections 793 (d) and (e) prohibit passing information to someone "not entitled to receive" it, but this term, as with the others, is not defined. The legislative history of the 1917 Act struck down a provision that would have allowed the President to determine who was entitled; therefore, an Executive Order cannot be used to clear up the meaning of the phrase. The question is left begging — are you entitled to receive all information unless you are specifically prohibited (i.e., a foreign agent)? Are you entitled to receive any information unless specifically prohibited (i.e., any loyal citizen is entitled)? Or is there a middle ground (i.e., the press is entitled)?

The Ellsberg defense argued the only constitutional interpretation of the statute was that any citizen without a culpable intent was entitled to receive information.

Retention. §793(d) and (e) also prohibit retaining national defense information without proper authority. Again, the meaning is unclear. Even if not pushed to the logical absurdity that one may not retain one's memories, it could put a serious cramp in the style of the former government official's fondness for writing memoirs — a resource, by the way, which Congress and the public make good use of. If what Congress actually had in mind was the custody of government papers, the statute should say so.

Activities Prior to Publication. The government avoided the most sensitive First Amendment issues by basing the Ellsberg/Russo indictment not on the transfer of the Pentagon Papers to Sen. Fulbright or to the *New York Times*, but on Ellsberg's giving the documents to Russo as they xeroxed them. In other words, they were indicted for an activity that was part of the necessary chain of events leading to their publication, and it seems safe to say that without their ultimate publication, the Ellsberg/Russo indictment never would have been brought. Yet Congress in 1917 rejected the Wilson administration's effort to make publication of national defense information a crime. Given the legislative history and First Amendment protections, is it possible that they intended to make illegal the actions which are necessary prior to publication?

In those specific situations where Congress has intended that publication be illegal, as with troop movements, codes, and atomic energy information, they have drawn the restrictions narrowly and have made their intentions clear. It seems more likely that the administration has taken advantage of the ambiguity in the statute.

S.1 — A Non-Solution

Since the S.1 espionage provisions are dead, there is little point in a detailed analysis of what was wrong with them. But they are instructive still because they provide a catalogue of what should be avoided. They are even more loosely drawn than the current statutes as to the kind of information protected, culpable intent behind its release, and recipients "not entitled to receive." The bill would have resolved all ambiguities in the statute in favor of still less disclosure. "Foreign power," for example, is redefined to include such international organizations as the United Nations, the Universal Postal Union, the World Health Organization, etc., and passing information to them which might work to their advantage — without even assuming that the information would be passed to foreign governments — would violate §1121 of S.1.

But worse still is that these "reforms" do not respond to the critical need for a counterbalance to a secrecy system which stifles public debate and insulates government officials from being called into account for their actions. Instead, the provisions of S.1 would have protected official crime with the same zeal that it would have protected other official secrets. Yet there is no indication why these laws to chill public debate are justified at this point in time; there is no indication, for example, that the current laws are allowing spies to escape.

And S.1 would have expanded the range of punishable activities alarmingly. It would have changed the scienter to include publication — merely "knowing" that the information "may be used to the prejudice . . . of the United States" would be enough to bring down criminal sanctions on the public spirited. The only material safe for publication and discussion would be information which had been *officially* released.

With the information available for public debate limited to the narrow range of officially sanctioned topics, the S.1 provisions cry out for constitutional challenge.

Alternative Proposals for Reforming the Current Espionage Laws

In response to the S.1 threat, several bills to reform the espionage laws have been presented to Congress as alternatives. These bills — introduced by Rep. Robert Kastenmeier (H.R. 10850, which represents the ACLU's recommendations), Sen. Philip Hart, and Sen. Birch Bayh — are briefly discussed below.

Type of Information Protected. The Kastenmeier/ACLU, Hart and Bayh bills all specify that the information must be properly classified and not in the public domain; the Hart and Bayh bills give a long list, drawn from the S.1 provisions, of categories of classified information subject to the espionage statutes. The Kastenmeier/ACLU bill narrows the range of protected information dramatically, to include only technical information about military operations in time of war, technical details of weaponry, and defensive military contingency plans. The Bayh and Hart bills include protection for a limited category called "Vital Defense Secrets" dealing with information which would cause "direct, immediate, and irreparable harm" to the national defense. In the Hart bill, the press would be subject to prosecution, a position which the ACLU faults because its standard is too vague to give fair notice of exactly what is prohibited.

Culpability. All three bills would require intent to injure the United States. In addition, the Hart bill retains the "reason to believe" and "advantage" language of the current statutes, but narrows "advantage" to mean "advantage to the national defense of a foreign power." The Bayh bill removes the "reason to believe" language of the current statutes, but keeps the injury/advantage language unchanged. The Kastenmeier/ACLU bill offers the most limited culpability standard — intent that the information "be used by a foreign nation to injure the national defense."

Recipient. Where S.1 renders virtually everyone unauthorized to receive any national defense information, these three bills all would limit the unauthorized recipient to foreign powers or their agents. The Hart bill specifically authorizes release of information to any member of Congress; based on the belief that the public has interests in information which are separate from those of Congress, the Kastenmeier/ACLU bill goes a step further and makes disclosure to either Congress or the public a defense to a prosecution.

Conclusion

The government persists in its interpretation of current law. Its testimony on behalf of S.1 argued that it simply codified present law (a position accepted by the majority of the Senate Judiciary Subcommittee reporting S.1) and the military has indicted and convicted a sergeant under §793(d), without alleging intent to injure the United States.

In spite of the welter of uncertainties about the meaning of the current espionage statutes, one factor emerges clearly — they are susceptible to sweeping interpretations which threaten the First Amendment. Because the Ellsberg/Russo case was dismissed, none of the legal ambiguities were resolved.

There remains a need for legislation which takes into account the lessons of Watergate and Vietnam — that it is essential for the public and Congress to know what the administration is doing and to participate in making major policy decisions. New statutes should take into account that there is more involved in the national security than the often claimed but seldom realized possibility that information might in some sense prejudice the interests of the government; such information can also be of vital importance to public and congressional participation in the policy making process. A new balance must be struck.

But as it now stands, the current espionage statutes remain on the books, and the administration's advocates continue to insist that they mean whatever the executive says they mean. All that stands between this and executive branch control of policy debate is the present gloss of judicial interpretation on how the statutes relate to espionage agents. The time has come for Congress to remove the uncertainty and enact legislation which is clearly meant to deter spies without encroaching on domestic political debate.

Illegal Intelligence Programs: Notifying the Victims

BY WENDY WATANABE and CHRISTINE M. MARWICK

There is now an extensively documented record of illegal surveillance and harassment carried out by the intelligence community, yet many of the victims remain unaware that they were the subjects of such programs. As a step toward remedying the effects of its own programs, the intelligence community could notify the targets of its mail openings, disruption tactics, warrantless electronic surveillances, burglaries, and other discredited programs, and advise them that they have rights under existing laws—the Freedom of Information Act provides access to files, the Privacy Act allows the amending of inaccurate and irrevelant records, and, on the basis of what is learned under these acts, victims could consider suing for damages and additional release.

Given this situation, where does the government currently stand on the question of notification?

The Chief Executive: President Ford

The Office of the President is apparently uninterested in the question. On October 30, 1975, the American Civil Liberties Union, the Center for National Security Studies and five other organizations sent a joint letter to President Ford requesting that he take the initiative and notify those individuals who had been victims of programs and advise them of their rights in court.

President Ford has not yet responded to the letter, nor has he publicly discussed the issue of notification.

The Department of Justice: Attorney General Levi

Attorney General Levi has been the first executive branch official to do something about the problem of notification. On April first, Levi announced the establishment of a special review committee to notify some subjects of COINTELPRO activities. Set up within the Justice Department's Office of Professional Responsibility, the "COINTELPRO Notification Program" includes the following policies:

- Subjects of improper actions which may have caused actual harm should be notified; doubts should be resolved in favor of notification.
- Those individuals who are already aware that they were subjects of COINTELPRO will not be notified.
- In each case, the manner of notification should protect the subject's right to privacy.
- Notification should be given as the work of the committee proceeds, without waiting for the entire review to be completed.
- Where appropriate, the committee should refer matters to the Criminal or Civil Rights Division for disciplinary action.
- No departure from these policies can be made without the express approval of the Attorney General.

Congress: The House

Rep. Bella Abzug, Chairwoman of the House Subcommittee on Government Information and Individual Rights, introduced a notice bill (H.R. 12039) on February 24, 1976 and has held hearings on the bill. In opening the hearings, she observed that the Department of Justice's decision to notify COINTELPRO victims is "far too narrow in scope and purpose"—COINTELPRO was only one of many documented programs which violated the rights of Americans. And while a notification program limited to COINTELPRO victims might be seen as an experiment, in itself it does nothing to respond to the problems of the victims of other extensive programs, such as the CIA's Operation CHAOS, illegal wiretaps, mail opening, or the IRS Special Services Staff. These latter programs are covered by the Abzug bill.

The Subcommittee took testimony from Director of Central Intelligence George Bush on April 28th, Bush opposed a notification program, maintaining that it would be be impossible to identify and locate the people involved, and "simply unnecessary" because the volume of requests under the Freedom of Information and Privacy Acts indicates that the public is already aware of its right to access. But Bush did not deal with the problem that the records contain information on many people who would not have expected a CIA file on them, or who would hesitate to open a file under the FOI/PA when the agency may not have an investigatory file on them.

The May 11th testimony from IRS Commissioner Donald C. Alexander and Deputy Assistant Secretary of Defense David O. Cooke argued that the Privacy Act amendments requiring notification were impractical, expensive, time consuming, and in conflict with existing law. Cooke also faulted the amendments for being overbroad —they would open investigative files to foreign nationals and "jeopardize our intelligence efforts."

Further hearings, from witnesses favoring rather opposing notification, are planned for June 3rd.

Congress: The Senate

The Senate Select Committee on Intelligence Activities has also advised extending Attorney General Levi's COINTELPRO notification program, and recommended in Book II of its Final Report that the government take responsibility for notifying all targets of illegal intelligence programs:

> Recommendation 90. The Freedom of Information Act (5 U.S.C. 552(b) and the Federal Privacy Act (5 U.S.C. 552(a)) provide important mechanisms by which individuals can gain access to information on intelligence activity directed against them. The Domestic Intelligence Recommendations assume that these statutes will continue to be vigorously enforced. In addition, the Department of Justice should notify all readily identifiable targets of past illegal surveillance techniques, and all COINTELPRO victims, and third parties who had received anonymous COINTELPRO communications, of the nature of the activities directed against them, or the source of the anonymous communication to them." *(Book II, p. 336)*

Conclusion

Given what we now know about the programs of the intelligence agencies, it is a logical step for the government to assume responsibility and institute a program for accountability. Notifying the subjects of such programs is a beginning; no one should have to guess whether he or she was the object of discredited government programs.

Reforming the Intelligence Agencies: Recommendations of the Senate Select Committee on Intelligence Activities

The following recommendations are reprinted from *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, United States Senate, Report No. 94-755, 94th Congress, 2d Session, April 26, 1976.

Book I — Foreign and Military Intelligence

Recommendation 35.—The legislation establishing the charter for the Central Intelligence Agency should specify that the CIA is the only U.S. Government agency authorized to conduct covert actions. The purpose of covert actions should be to deal with grave threats to American security. Covert actions should be consistent with publicly-defined United States foreign policy goals, and should be reserved for extraordinary circumstances when no other means will suffice. The legislation governing covert action should require executive branch procedures which will ensure careful and thorough consideration of both the general policies governing covert action and particular covert action projects; such procedures should require the participation and accountability of highest level policymakers.

Recommendation 36.—The Committee has already recommended, following its investigation of alleged assassination attempts directed at foreign leaders, a statute to forbid such activities. The Committee reaffirms its support for such a statute and further recommends prohibiting the following covert activities by statute:

- All political assassinations.
- Efforts to subvert democratic governments.
- Support for police or other internal security forces which engage in the systematic violation of human rights.

Recommendation 37.—By statute, the appropriate NSC committee (e.g., the Operations Advisory Group) should review every covert action proposal.

The Committee recommends that the Operations Advisory Group review include:

- A careful and systematic analysis of the policital premises underlying the recommended actions, as well as the nature, extent, purpose, risks, likelihood of success, and costs of the operation. Reasons explaining why the objective cannot be achieved by overt means should also be considered.
- Each covert action project should be formally considered at a meeting of the OAG, and if approved, forwarded to the President for final decision. The views and positions of the participants would be fully recorded. For the purpose of OAG, presidential, and congressional considerations, all so-called non-sensitive projects should be aggregated according to the extraordinary circumstances of the contingency against which the project is directed.

Recommendation 38.—By statute, the intelligence oversight committee(s) of Congress should require that the annual budget submission for covert action programs be specified and detailed as to the activity recommended. Unforeseen covert action projects should be funded from the Contingency Reserve Fund which could be replenished only after the concurrence of the oversight and any other appropriate congressional committees. The congressional intelligence oversight committees should be notified prior to any withdrawal from the Contingency Reserve Fund.

Recommendation 39.—By statute, any covert use by the U.S. Government of American citizens as combatants should be preceded by the notification required for all covert actions. The statute should provide that within 60 days of such notifica-

tion such use shall be terminated unless the Congress has specifically authorized such use. The Congress should be empowered to terminate such use at any time.

Recommendation 40.—By statute, the executive branch should be prevented from conducting any covert military assistance program (including the indirect or direct provision of military material, military or logistics advice and training, and funds for mercenaries) without the explicit prior consent of the intelligence oversight committee(s) of Congress.

Recommendation 42.—The Committee is concerned about the integrity of American institutions and the use of individuals affiliated with such institutions for clandestine purposes. Accordingly, the Committee recommends that the CIA amend its internal directives to require that individual academics used for operational purposes by the CIA, together with the President or equivalent official of the relevant academic institutions, be informed of the clandestine CIA relationship.

Recommendation 43.—The Committee further recommends that, as soon as possible, the permanent intelligence oversight committee(s) of Congress examine whether further steps are needed to insure the integrity of American academic institutions.

Recommendation 44.—By statute, the CIA should be prohibited from the operational use of grantees who are receiving funds through educational and/or cultural programs which are sponsored by the United States Government.

Recommendation 45.—By statute, the CIA should be prohibited from subsidizing the writing, or production for distribution within the United States or its territories, of any book, magazine, article, publication, film, or video or audio tape unless publicly attributed to the CIA. Nor should the CIA be permitted to undertake any activity to accomplish indirectly such distribution within the United States or its territories.

Recommendation 46.—The Committee supports the recently adopted CIA prohibitions against any paid or contractual relationship between the Agency and U.S. and foreign journalists accredited to U.S. media organizations. The CIA prohibitions should, however, be established in law.

Recommendation 47.—The Committee recommends that the CIA prohibitions be extended by law to include the operational use of any person who regularly contributes material to, or is regularly involved directly or indirectly in the editing of material, or regularly acts to set policy or provide direction to the activities of U.S. media organizations.

Recommendation 48.—The Committee recommends that the Agency's recent prohibition on covert paid or contractual relationship between the Agency and any American clergyman or missionary should be established by law.

Book II — Intelligence Activities and the Rights of Americans

Recommendation 1.—There is no inherent constitutional authority for the President or any intelligence agency to violate the law.

Recommendation 2.—It is the intent of the Committee that statutes implementing these recommendations provide the exclusive legal authority for federal domestic security activities.

(a) No intelligence agency may engage in such activities unless authorized by statute, nor may it permit its employees, informants, or other covert human sources to engage in such activities on its behalf.

(b) No executive directive or order may be issued which would conflict with such statutes.

Recommendation 16.—NSA should not be permitted to select for monitoring any communication to, from, or about an American without his consent, except for the purpose of obtaining information about hostile foreign intelligence or terrorist activities, and then only if a warrant approving such monitoring is obtained in accordance with procedures similar to those contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Recommendation 27.—The IRS should not, on behalf of any intelligence agency or for its own use, collect any information about the activities of Americans except for the purposes of enforcing the tax laws.

Recommendation 28.—IRS should not select any person or group for tax investigation on the basis of political activity or for any other reason not relevant to enforcement of the tax laws.

Recommendation 42.—The FBI should be permitted to investigate a committed act which may violate a federal criminal statute pertaining to the domestic security to determine the identity of the perpetrator or to determine whether the act violates such a statute.

Recommendation 43.—The FBI should be permitted to investigate an American or foreigner to obtain evidence of criminal activity where there is "reasonable suspicion" that the American or foreigner has committed, is committing, or is about to commit a specific act which violates a federal statute pertaining to the domestic security.

Recommendation 44.—The FBI should be permitted to conduct a preliminary preventive intelligence investigation of an American or foreigner where it has a specific allegation or specific or substantiated information that the American or foreigner will soon engage in terrorist activity or hostile foreign intelligence activity. Such a preliminary investigation

should not continue longer than thirty days from receipt of the information unless the Attorney General or his designee finds that the information and any corroboration which has been obtained warrants investigation for an additional period which may not exceed sixty days. If, at the outset or at any time during the course of a preliminary investigation the Bureau establishes "reasonable suspicion" that an American or foreigner will soon engage in terrorist activity or hostile foreign intelligence activity, it may conduct a full preventive intelligence investigation. Such full investigation should not continue longer than one year except upon a finding of compelling circumstances by the Attorney General or his designee.

In no event should the FBI open a preliminary or full preventive intelligence investigation based upon information that an American is advocating political ideas or engaging in lawful political activities or is associating with others for the purpose of petitioning the government for redress of grievances or other such constitutionally protected purpose.

Recommendation 51.—All nonconsensual electronic surveillance, mail-opening, and unauthorized entries should be conducted only upon authority of a judicial warrant.

Recommendation 52.—All nonconsensual electronic surveillance should be conducted pursuant to judicial warrants issued under authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

The Act should be amended to provide, with respect to electronic surveillance of foreigners in the United States, that a warrant may issue if

(a) There is probable cause that the target is an officer, employee, or conscious agent of a foreign power.

(b) The Attorney General has certified that the surveillance is likely to reveal information necessary to the protection of the nation against actual or potential attack or other hostile acts of force of a foreign power; to obtain foreign intelligence information deemed essential to the security of the United States; or to protect national security information against hostile foreign intelligence activity.

(c) With respect to any such electronic surveillance, the judge should adopt procedures to minimize the acquisition and retention of nonforeign intelligence information about Americans.

(d) Such electronic surveillance should be exempt from the disclosure requirements of Title III of the 1968 Act as to foreigners generally and as to Americans if they are involved in hostile foreign intelligence activity.

As noted earlier, the Committee believes that the espionage laws should be amended to include industrial espionage and other modern forms of espionage not presently covered and Title III should incorporate any such amendment. The Committee's recommendation is that both that change and the amendment of Title III to require warrants for all electronic surveillance be promptly made.

Recommendation 66.—Information previously gained by the FBI or any other intelligence agency through illegal techniques should be sealed or purged as soon as practicable.

Recommendation 90.—The Freedom of Information Act (5 U.S.C. 552(b)) and the Federal Privacy Act (5 U.S.C. 522(a)) provide important mechanisms by which individuals can gain access to information on intelligence activity directed against them. The Domestic Intelligence Recommendations assume that these statutes will continue to be vigorously enforced. In addition, the Department of Justice should notify all readily identifiable targets of past illegal surveillance technqiues, and all COINTELPRO victims, and third parties who had received anonymous COINTELPRO communications, of the nature of the activities directed against them, or the source of the anonymous communication to them.

Recommendation 91.—Congress should enact a comprehensive civil remedies statute which would accomplish the following:

(a) Any American with a substantial and specific claim to an actual or threatened injury by a violation of the Constitution by federal intelligence officers or agents acting under color of law should have a federal cause of action against the government and the individual federal intelligence officer or agent responsible for the violation, without regard to the monetary amount in controversy. If actual injury is proven in court, the Committee believes that the injured person should be entitled to equitable relief, actual, general, and punitive damages, and recovery of the costs of litigation. If threatened injury is proven in court, the Committee believes that equitable relief and recovery of the costs of litigation should be available.

(b) Any American with substantial and specific claim to actual or threatened injury by violation of the statutory charter for intelligence activity (as proposed by these Domestic Intelligence Recommendations) should have a cause of action for relief as in (a) above.

(c) Because of the secrecy that surrrounds intelligence programs, the Committee believes that a plaintiff should have two years from the date upon which he discovers, or reasonably should have discovered, the facts which give rise to a cause of action for relief from a constitutional or statutory violation.

(d) Whatever statutory provision may be made to permit an individual defendant to raise an affirmative defense that he acted within the scope of his official duties, in good faith, and with a reasonable belief that the action he took was lawful, the Committee believes that to ensure relief to persons injured by governmental intelligence activity, this defense should be available solely to individual defendants and should not extend to the government. Moreover, the defense should not be available to bar injunctions against individual defendants.

Recommendation 93.—Congress should either repeal the Smith Act (18 U.S.C. 2385) and the Voorhis Act (18 U.S.C. 2386), which on their face appear to authorize investigation of "mere advocacy" of a political ideology, or amend those statutes so that domestic security investigations are only directed at conduct which might serve as the basis for a constitutional criminal prosecution, under Supreme Court decisions interpreting these and related statutes.

		PRICE (PREPAID)	QUANTITY	TOTAL
NEWSLETTER	First Principles (published monthly except July and August). List of back issues—free.	$15/year regular		
		$5/year student		
FOIA	How to Get Your Personal File	50¢ first copy		
PUBLICATIONS		25¢ ea. add'l copy		
	The New Freedom of Information Act and National Security Secrecy	50¢ first copy		
		25¢ ea. add'l. copy		
	Abstracts of Documents Released under the FOIA (includes order blank for documents)	$1.40		
ARTICLES	*Led Astray by the CIA*, and other articles By Morton H. Halperin	$1.00		
	National Security and Civil Liberties. By Morton H. Halperin	50¢		
BOOKS	*Litigation Under the Amended Federal Freedon of Information Act*, Edited by Christine M. Marwick, 218 pages. Technical manual for attorneys.	$20/copy: attorneys, institutions, government $5/copy: pub. int. organizations, law faculty, students		
	The CIA and the Cult of Intelligence. Victor Marchetti and John Marks	$1.75, paper; $10 autographed hardcover		
	The CIA File, ed. Robt. Borosage & John Marks. Articles analyzing implications of CIA domestic and foreign policies	$8.95 hardcover		
		PREPAID	*Total*	

PUBLICATIONS AVAILABLE FROM THE PROJECT ON NATIONAL SECURITY AND CIVIL LIBERTIES

122 Maryland Avenue, N.E., Washington, D.C. 20002

PREPAID: Make checks for publications payable to the Project

Contributions to the Project are tax deductible; they should be made out to either the American Civil Liberties Union Foundation or the Fund for Peace, c/o Project on National Security and Civil Liberties, 122 Maryland Avenue, N.E., Washington, D.C. 20002

SEND TO:

Name

Address

City *State* *Zip*

Please fill out mailing label

Point Of View

(continued from page 16)

Since espionage, sabotage, and terrorism are violations of the law, Congress should require that the Justice Department wiretap, if at all, only under the existing procedures for criminal investigations. For activity which is not now criminal, Congress should consider whether such conduct should be made criminal and should then determine whether it justifies electronic surveillance. The new proposed procedures should apply only to foreign powers and their foreign employees.

The second major issue comes in the bill's last section which amounts to a disclaimer clause. It states that nothing in the bill "shall limit the constitutional power of the President to order electronic surveillance . . . if the facts and circumstances giving rise to such order are beyond the scope of this chapter."

If there is to be any provision for surveillance outside the procedures in the bill, Congress should define precisely what "facts and circumstances" might allow it (i.e., international communications in situations imminently dangerous to our country). Levi conceded that the disclaimer clause left open the possibility for conducting domestic surveillances when he promised that he would not use that authority. But since Congress can appropriately legislate in the area of electronic surveillance and can define the procedures for all "national security" wiretaps, why should it surrender this responsibility in an ambiguous and overly broad disclaimer clause?

One unstated purpose of the disclaimer clause is to permit the National Security Agency to continue its "sweep" operations that monitor overseas phone calls and telegrams. Such monitoring should be banned or at least be conducted only under warrant procedures, but there are complex issues involved and Congress might reasonably deal with this specific issue in separate legislation. If this is the case, then Congress should say so, rather than legislating a general disclaimer, which opens the door to warrantless, domestic wiretaps.

Another motive behind the disclaimer is the belief that the President may require special powers to deal with crises that threaten the nation's survival. I find it difficult to believe that such a situation could not be handled within the emergency warrant procedures of the bill, but if (apart from the NSA problem) this is the disclaimer's only purpose, then Congress should say so explicitly. Such a provision could be in the form of an explicit grant of congressional authority in carefully delineated crises.

The time for legislative reform limiting national security wiretaps is long past due. The executive branch has now provided the vehicle; Congress can and should provide the procedural changes to make it a truly effective piece of legislation. Perhaps it will.

First Principles
is published by the
Project on National
Security and Civil
Liberties, which is
sponsored by the
American Civil Liberties
Union Foundation and the
Center for National
Security Studies of the
Fund For Peace.

122 Maryland Avenue, N.E., Washington, D.C. 20002
(202) 544-5380

Non-Profit Org.
U. S. Postage
PAID
Permit No. 45490
Washington, D.C.

Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger, real or pretended, from abroad.

JAMES MADISON TO THOMAS JEFFERSON,
MAY 13, 1798

Point of View

Warrants for Wiretaps

Morton H. Halperin

In response to continuing publicity about the abuse of asserted presidential power to conduct electronic surveillance without a warrant, Attorney General Levi has finally been persuaded to support legislation designed to remedy the problem. This bill, S. 3197 and its counterpart H.R. 12750, have been introduced on behalf of the administration by Senator Kennedy and Chairman Rodino of the House Judiciary Committee. The bills appear to be a substantial step forward, and indeed they could be.

But, as is often the case in reform proposals, what is granted as a general principle is then taken away in the fine print. The same pattern was used in the executive order purporting to control the intelligence agencies (see *First Principles*, March 1976). The broad prohibitions in the bill appear to have been written by senior officials and the exceptions added by technicians. And as with the executive order, the fine print could actually allow the executive branch even more freedom for warrantless electronic surveillance.

A number of the minor loopholes in the bill have been exposed and seem to be on the way to resolution. For example, the proposed legislation would have lifted the civil and the criminal penalties which now apply to all illegal or unconstitutional electronic surveillance.

Two major problems remain, and the legislation will be a step forward only if they are resolved. The first is the continued potential for surveillance of American citizens, and the second is the continued claim of presidential power to wiretap beyond the restrictions set out by the proposed legislation.

On the first issue, if the government (including the President) has any right at all to wiretap American citizens in any circumstances, it should be limited to situations in which a warrant is issued based on probable cause to believe that a crime has been or is about to be committed. Any other standard is open to abuse and provides no effective check on executive power.

The legislation as presently drafted, however, permits the government to conduct electronic surveillance of American citizens who are not engaged in crime, but who are "assisting" a foreign political "faction" or "party" in something called "clandestine intelligence activities." The Attorney General has said explicitly that this includes activities which are not illegal under federal law. As examples, he cites collection of information from industry, activities directed against foreign installations in the United States, or arson committed in a state capital building. But without a concise definition of what constitutes "clandestine intelligence activities," the bill opens the door for the kind of domestic spying it purports to curb.

(continued on page 15)

Collective Impressions Printshop
1436 R Street, NW
Washington, DC 20009
234-4118

Typesetting by
Unicorn Graphics,
Silver Spring, Md.